Are you keeping
credit card information safe?
Maybe not — if you keep it on file

By Miles Bodzin, DC

Running a cash practice is not new to our profession. But many doctors who run a cash practice — especially those whose patients are on a prepayment plan — are engaging in a problematic procedure — keeping patients’ credit cards on file so they can perform an auto-debit.

Storing cardholder data (credit card numbers) in a log book, file cabinet, tickler-reminder system, or spreadsheet with the purpose of entering them into a credit card machine every month is a clear violation of Payment Card Industry Data Security Standards (PCI DSS).

If you can retrieve the full account number from the system you use, then your filing system is not PCI DSS-compliant and your company is subject to security breaches.

WHY SHOULD YOU CARE?
You probably learned from recent headlines that stolen credit and debit card data due to security breaches at businesses — both large and small — have negatively impacted millions of consumers. The data thieves are both hackers and employees.

To protect merchants and consumers, the major card brands, including Visa and MasterCard, established the PCI DSS to help ensure the integrity of the card system. The PCI DSS spells out security guidelines to help businesses minimize the possibility of a data security breach in their card-processing systems.

PCI DSS is to the credit card industry as HIPAA is to healthcare industry — established to protect consumers.

You may not be aware, but since June 2005, merchants (such as you) have been required to follow PCI DSS or face hefty fines in the event of a security breach. If there is fraudulent use of card data, you can be financially responsible — and the fines can be as high as $25,000 per incident. Visa, one of the largest credit card companies, fined merchants millions of dollars last year.

You don’t have to be a large company to have a security breach. In fact, hackers and thieves know that small businesses, such as chiropractic offices, are more likely to be unaware of the standard and therefore become easy targets for data theft.

If the way you process, transmit, or store cardholder data could result in breaches of cardholder data security without your knowledge, you are vulnerable. You can overcome your vulnerability, however, by using PCI DSS compliant software and ensuring you do not store credit card numbers in any other way.
PCI DSS' core standards and requirements

- PCI DSS-compliance standards include the following requirements and are developed around a core of principles:
  - **Build and maintain a secure network.** To achieve this, users are required to install and maintain a firewall configuration to protect cardholder data. Additionally, they are not to use vendor-supplied defaults for system passwords and other security parameters.
  - **Protect cardholder data.** Vendors are required to protect stored cardholder data and to encrypt transmission of cardholder data across open, public networks.
    - **Maintain a vulnerability management program.** Vendors must use and regularly update their antivirus software, and develop and maintain secure systems and applications.
    - **Implement strong access-control measures.** Users must restrict access to cardholder data by business need-to-know, assign a unique ID to each person with computer access, and restrict physical access to cardholder data.
  - **Regularly monitor and test networks.** Vendors who agree to follow the standard must track and monitor all access or network resources and cardholder data. They must also regularly test their security systems and processes.
  - **Maintain an information-security policy.** Users agree to maintain a policy that addresses information security.

For more information on the PCI DSS, visit www.pcisurencet.com.

On Oct. 9, 2007, Visa released a mandated timeline for merchants to eliminate vulnerable applications and ultimately to use only validated versions. This is a reflection of the heightened risk involved in applications that store credit card information.

It is your responsibility to ensure you are protecting your business from potentially dangerous security breaches. Miles Bodzin, DC, is CEO of Cash Practice, Inc., which provides PCI DSS-compliant auto-debiting software. He can be reached at 877-FIFTY-50. drbodzin@cashpractice.com, or at www.CashPractice.com.
“If insurance was gone tomorrow, would you survive in practice?”

If you’re not 100% sure, read on to learn how my company, Cash Practice® Systems, can help you not only survive but thrive in spite of a worsening insurance climate.

With all the uncertainty in health care insurance and “Obamacare”, there has never been a more important time for you to take decisive action to ensure your future success. For over a decade, our systems have helped thousands of doctors of chiropractic free themselves from the shackles of insurance dependence.

We can help you too! Our systems have one sole purpose - increase your patient retention and care plan compliance, resulting in freedom from insurance dependence. Nobody else even comes close to the retention levels we see. Our members routinely have PVA’s well over 100 visits.

Join us, and you will skyrocket your patient retention & cash collections, reduce your stress and help more people get well.

Membership Includes:

- The Wellness Score® System
- Cash Plan Calculator® System
- Auto-Debit System®
- Drip-Education® System
- Cash Practice. Mobile App
- Staff Bonus System
- Integrates with chirotouch ChiroHealthUSA

MILES BODZIN, DC
Founder & CEO

FREE DOWNLOAD of Amazon’s #1 Best Seller
SUCCESSONOMICS
Featuring Steve Forbes & Miles Bodzin, DC

Text your Name, Email & “CPART” to (619)609-0521

Join me every Tuesday at 10am PST for an Info-Packed Webinar
REGISTER AT CashPractice.com

For more information on how to free yourself from insurance dependence, email us at info@cashpractice.com or call (877)343-8950